Estudios y Perspectivas
Revista Científica y Académica
Fecha de recepción: 07/01/2024
Fecha de aprobación: 15/02/2024
DOI: https://doi.org/10.61384/r.c.a..v4i1.90

Seguridad de la Información y Ciberseguridad: Su Importancia para los Estados, Empresas y las Personas, Una Revisión Sistemática

Henry M. Rodríguez Zambrano
Ph. D. en Políticas Públicas
Organización de Estados Iberoamericanos
hrodriguez@contratista.oei.org.co
https://orcid.org/0009-0002-9819-8141
Carlos H. Moreno Tamayo
Administrador de Empresas y Administrador Policial
Organización de Estados Iberoamericanos
carlos.moreno@oei.int
https://orcid.org/0000-0002-2173-6098

RESUMEN

Este trabajo tuvo como objetivo identificar la importancia de la seguridad de la información, poniendo énfasis en la ciberseguridad en el ámbito nacional, empresarial y laboral, ante la necesidad de contar con herramientas para prevenir ser víctima de ciberataques. Se hizo una revisión de 15 documentos publicados desde el año 2015 hasta el 2022, con los cuales se realizó una triangulación de la información que permitió establecer un debate que abre posibles líneas de investigación para futuros trabajos. A partir de un enfoque *top-down* y de un ejercicio exploratorio-descriptivo, se hizo una revisión sistemática de la información, lo que permitió llegar a la identificación del papel crucial de la ciberseguridad en el funcionamiento del mundo actual.

Palabras clave: *Ciberseguridad, cooperación, educación, inversión en tecnología, seguridad de la información.*

Information Security and Cybersecurity: Its Importance for States, Companies and People, A Systematic Review

ABSTRACT

This work aimed to identify the importance of information security, with an emphasis on cybersecurity at the national, corporate, and workplace levels, and the need for tools to prevent cyberattacks. A review of 15 documents published from 2015 to 2022 was conducted, enabling the researchers to triangulate all existing information, and thus, to facilitate a discussion that opens up new lines of research for future studies. Using a top-down approach and an exploratory-descriptive exercise, a systematic review of information was carried out, leading to the recognition of the crucial role of cybersecurity in the functioning of the modern world.

Keywords: *Cybersecurity, cooperation, education, investment in technology, information security.*

INTRODUCCIÓN

La ciberseguridad es fundamental en un mundo cada vez más digital. Gobiernos de Europa, Estados Unidos y Latinoamérica diseñan e implementan estrategias de prevención y defensa contra ciberataques, mientras que empresas e individuos se encuentran en condición de vulnerabilidad frente a diversas técnicas usadas por los atacantes, debido, fundamentalmente, al escaso nivel de conciencia. Así, desde una perspectiva global hasta el ámbito individual, se observa una creciente necesidad de comprender y abordar las amenazas cibernéticas. Por esto, científica y tecnológicamente es necesario conocer, comprender y afrontar estos desafíos evaluando las estrategias existentes y proponiendo enfoques más efectivos para proteger la información en un entorno digital en constante evolución.

En este sentido, este artículo de revisión sistemática tiene como objetivo comprender el papel que tiene la seguridad de la información, poniendo el acento en la ciberseguridad. En este sentido, se aborda cómo debe ser implementada por los gobiernos, empresas, organizaciones, hasta llegar al ámbito ciudadano.

MATERIALES

El marco temporal de esta revisión comprende desde el 2015 hasta el 2022. La recolección de la información se realizó de manera documental, haciendo un barrido inicial por el buscador Google Académico y las bases de datos Scielo y Dialnet, de los que se seleccionó un total de 15 documentos que, dadas sus características, cumplen los requisitos necesarios para ser tomados como fuentes de información confiables.

Metodológicamente, se hizo un ejercicio exploratorio-descriptivo, desde un enfoque *top*-down (descendente), promovido en la década de 1970 por los investigadores de IBM Harlan Mills y Niklaus Wirth, y en el que un equipo o gerente de proyectos toma decisiones que luego se transmiten a través de una estructura jerárquica.

Esta metodología en la investigación de ciberseguridad se basa en un enfoque exploratorio-descriptivo, en el que se parte de una visión global o de alto nivel para luego desglosar y analizar los detalles específicos.

Tal enfoque permite una comprensión integral de los sistemas y las estrategias de seguridad, identificando primero los aspectos clave antes de profundizar en los detalles, lo que resulta en una visión más completa y efectiva de la ciberseguridad.

En particular, para el análisis de la información, se prestó atención a los resultados principales, las limitaciones de los estudios y las conclusiones de los autores.

CRITERIOS DE INCLUSIÓN

Se consideraron cinco criterios de inclusión para la revisión sistemática en ciberseguridad:

1. Tipo de fuente: Se incluyeron publicaciones en revistas indexadas, informes técnicos, documentos de trabajo y libros relacionados con la ciberseguridad. Esta ampliación permitirá abarcar una variedad de fuentes de información relevantes.

2. Período de publicación: Se consideraron documentos publicados desde el año 2015 hasta la fecha actual, lo que garantizó la inclusión de investigaciones recientes y relevantes en el campo de la ciberseguridad.

3. Idioma: Se admitieron publicaciones en inglés y español, con el objetivo de abarcar un espectro más amplio de literatura en ciberseguridad. Esto permitió la inclusión de investigaciones importantes en múltiples idiomas.

4. Ámbito geográfico: La revisión se centró en investigaciones y publicaciones a nivel internacional, sin restricciones geográficas, para proporcionar una perspectiva global de la ciberseguridad.

5. Nivel de acceso: Se incluyeron publicaciones de acceso abierto siempre y cuando la versión completa esté disponible a través de bibliotecas académicas o institucionales. Esto amplió el alcance de la revisión y permitió la inclusión de investigaciones valiosas, incluso si requería acceso a través de suscripción.

CRITERIOS DE EXCLUSIÓN

Se consideraron cinco criterios de exclusión para la revisión sistemática en ciberseguridad:

1. Publicaciones no relacionadas: Se excluyeron aquellas publicaciones que no estén directamente relacionadas con la ciberseguridad o que no aborden temas pertinentes dentro de este campo.

2. Período de publicación: Se excluyeron todos los documentos publicados antes del año 2015, con el fin de evitar información extemporánea o sin vigencia actual.

3. Idioma no admitido: Se excluyeron publicaciones en idiomas diferentes al inglés y español, para mantener la coherencia y la comprensión de las fuentes incluidas.

4. Ámbito geográfico: Se excluyeron publicaciones que se centren exclusivamente en la ciberseguridad en regiones geográficas que no sean de interés para la investigación, a menos que proporcionen información de relevancia global.

5. Fuentes no disponibles: Se excluyeron publicaciones que no estuvieran disponibles a través de acceso abierto o a través de bibliotecas académicas o institucionales, a menos que se pudiera obtener acceso de manera legítima sin restricciones significativas.

En la tabla 1, se presentan las categorías de análisis y se incluyen algunos elementos de análisis por cada categoría.

Tabla 1 Matriz de fuentes

Tema	Autor	Año	País	Categorías
Ciberseguridad	Carlos Arturo Castillo Medina	2021	Colombia	La ciberseguridad y sus escenarios de aplicación: la importancia de los sistemas de información, y de un enfoque sistémico.
Riesgos y amenazas de internet a la seguridad humana	Rafael Rodríguez Prieto	2016	España	Internet y la sociedad: las implicaciones éticas del manejo de la información.
Ciberseguridad en el contexto internacional	David Ramírez Morán	2015	España	El estado de la ciberseguridad en las naciones: comparación de diversos informes.
Iniciativa nacional para la educación en ciberseguridad	Rodney Petersen; Danielle Santos; Karen A. Wetzel; Matthew C. Smith; Greg Witte	2020	Estados Unidos	Concienciación sobre la ciberseguridad: normas sobre educación en ciberseguridad.
Compendio de ciberdelincuencia	Naciones Unidas	2022	Estados Unidos	La ciberdelincuencia y las naciones: la necesidad de la

				cooperación entre naciones en temas de ciberseguridad.
Importancia de la ciberseguridad para las naciones	Agnese Carlini	2016	España	La necesidad de inversión en ciberdefensa: el conocimiento de las debilidades de los Estados en esta materia.
Estrategias nacionales de ciberseguridad	• Eduardo Alfredo Leiva	2015	Argentina	La penetración de las tecnologías de las comunicaciones y su impacto en los Estados: aspectos asociados a la vulnerabilidad y la ciberdelincuencia.
Desafíos en ciberseguridad	Milton Ricardo Ospina, Pedro Emilio Sanabria Rangel	2020	Colombia	La situación actual de Colombia en materia de ciberseguridad: identificación del escenario y los puntos vulnerables.
Ciberseguridad en Colombia	• Gladys Elena Medina Ochoa •	2020	Colombia	Cuál es la situación actual del país en esta materia con relación a la región: elementos para establecer una cooperación sólida con otros países.
Seguridad y ciberseguridad	Jeimy J. Cano M.	2020	Colombia	La evolución de las tecnologías de la comunicación en la sociedad: el avance de las amenazas a la seguridad de la información.
Seguridad de la información, ciberseguridad, estrategias de prevención	• José Manuel Ortega Candel	2021	España	Evaluación de la ciberseguridad: aplicación de un modelo de evaluación en ciberseguridad para instituciones.
Estrategia de protección en ciberseguridad	• Daniel Álvarez	2017	Chile	Ciberseguridad en Chile: los vacíos existentes en este tema en la legislación chilena.

Amenazas de ciberseguridad en empresas	● Enrique Javier Santiago, Jesús Sánchez Allende	2017	España	Riesgos de ciberseguridad de empresas: cuáles son las mejores estrategias que se pueden adoptar, cuál es el papel del capital humano.
El personal en las empresas y su relación con la ciberseguridad	● Luis Felipe Guillermo García Forero	2020	Colombia	Ciberseguridad, ingeniería social, *phishing* o suplantación, el usuario, el eslabón más débil en la cadena de la seguridad de la información.

MÉTODOS

La recolección de la información partió de una búsqueda de palabras clave como ciberseguridad, ciberdelitos, ciberseguridad empresas, ciberataque gobiernos.

Los operadores utilizados son AND, OR y NOT. Estos son operadores lógicos utilizados en búsquedas booleanas y consultas de búsqueda en bases de datos, motores de búsqueda en línea y sistemas de recuperación de información. Estos operadores permiten combinar términos o palabras clave para refinar una búsqueda y encontrar resultados más específicos o amplios, según sea necesario. Además, los parámetros utilizados son fecha, artículo, investigación.

La investigación documental contó con la elaboración de la ficha de registro, con el fin de definir categorías para los artículos analizados como se observa en la tabla 2. Se ofrece una visión general de la información que permite cotejar investigaciones sobre ciberseguridad efectuadas en diversos países de América Latina, en Colombia y en las empresas, lo que enriquece la visión de la situación estudiada.

Tabla 2 Ficha de registro

Título	Resumen	Palabras clave	Análisis	Conclusión
Ciberseguridad, por dónde empezar	El documento presenta una guía práctica para implementar medidas de ciberseguridad en organizaciones de cualquier tamaño.	Ámbitos de aplicación.	El autor aborda los aspectos clave de la ciberseguridad, como la gestión de riesgos, la seguridad de la información, la seguridad de las redes y la seguridad de los sistemas.	El autor proporciona información clara y concisa sobre los aspectos clave de la ciberseguridad, y las recomendaciones son fáciles de implementar.
¿Qué es seguridad? Riesgos y amenazas de Internet en la seguridad humana	El documento analiza los riesgos y amenazas que Internet representa para la seguridad humana.	Internet, seguridad, sociedad internacional, ciberguerra, riesgos.	El autor analiza los riesgos y amenazas que Internet representa para la seguridad humana, incluyendo la ciberguerra, el ciberterrorismo, la ciberdelincuencia y la pérdida de privacidad.	El autor propone un enfoque basado en la cooperación internacional y la participación ciudadana para garantizar la seguridad humana en el ciberespacio.
La visión internacional de la ciberseguridad	El autor argumenta que la ciberseguridad es un problema global que requiere una respuesta internacional coordinada.	Ciberseguridad, seguridad internacional, ciberataques, cooperación internacional.	El autor proporciona una perspectiva general completa de la visión internacional de la ciberseguridad. El análisis es equilibrado y proporciona información valiosa para la comprensión de este tema.	El autor propone una serie de medidas para mejorar la cooperación internacional, incluyendo el intercambio de información, la formación conjunta y la creación de mecanismos de respuesta a incidentes.
Iniciativa nacional para la educación en ciberseguridad (NICE): marco para el personal de ciberseguridad	El marco define las habilidades y competencias necesarias para el personal de ciberseguridad, y proporciona una guía para el desarrollo de programas de formación y educación.	Ciberseguridad, educación, formación, habilidades, competencias.	El marco es claro y conciso, y proporciona información valiosa para la comprensión de las habilidades y competencias necesarias para el personal de ciberseguridad.	El marco proporciona una guía para el desarrollo de programas de formación y educación, incluyendo los objetivos, los contenidos y los métodos de enseñanza y aprendizaje.

Compendio de ciberdelincuencia	El compendio incluye casos de ciberataques, ciberespionaje y otros delitos cibernéticos cometidos por grupos organizados.	Ciberdelincuencia, cibercrimen, delincuencia organizada, ciberataques, ciberespionaje.	El compendio es claro y conciso, y proporciona información valiosa para la comprensión de la ciberdelincuencia organizada.	El compendio proporciona información sobre las técnicas, los métodos y las motivaciones de los grupos organizados que cometen delitos cibernéticos.
Ciberseguridad: un nuevo desafío para la comunidad internacional	El documento examina las amenazas cibernéticas, las vulnerabilidades de las infraestructuras críticas y las posibles respuestas a la ciberseguridad.	Ciberseguridad, seguridad internacional, ciberataques, delincuencia organizada.	El autor proporciona una visión general completa de los desafíos que la ciberseguridad plantea a la comunidad internacional.	El autor propone una serie de medidas para mejorar la cooperación internacional, incluyendo el intercambio de información, la formación conjunta y la creación de mecanismos de respuesta a incidentes.
Estrategias nacionales de ciberseguridad: Estudio comparativo basado en enfoque *top-down* desde una visión global a una visión local	Estudio comparativo de las estrategias nacionales de ciberseguridad de 10 países, incluyendo Estados Unidos, Reino Unido, Francia, Alemania, España, China, Rusia, Brasil, México y Colombia.	Ciberseguridad, estrategias nacionales, *enfoque top-down*, visión global, visión local.	El estudio es completo y proporciona información valiosa para comprender las estrategias nacionales de ciberseguridad.	El estudio concluye que las estrategias nacionales de ciberseguridad comparten una serie de objetivos y principios, pero también existen diferencias significativas en su enfoque y contenido.
Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia	Este artículo analiza los desafíos nacionales frente a la ciberseguridad en Colombia, en un contexto global.	● Ciberseguridad , ● seguridad de la información, ● amenazas cibernéticas ● Colombia.	Los autores abordan los aspectos históricos, conceptuales, normativos y técnicos de la ciberseguridad, y ofrecen una visión actualizada de la situación en Colombia.	El artículo concluye que Colombia debe fortalecer su capacidad de respuesta a las amenazas cibernéticas.

La seguridad en el ciberespacio: un desafío para Colombia	● Los autores abordan los conceptos de ciberseguridad y ciberdefensa, y destacan la importancia de la cooperación entre el sector público y privado para afrontar las amenazas cibernéticas.	Ciberseguridad, ciberdefensa, amenazas cibernéticas Colombia.	Los autores abordan los aspectos conceptuales, normativos y técnicos de la ciberseguridad, y ofrecen una visión actualizada de la situación en Colombia.	El documento concluye que Colombia debe fortalecer su capacidad de respuesta a las amenazas cibernéticas.
Seguridad y ciberseguridad 2009-2019.	Este artículo analiza las principales tendencias en seguridad y ciberseguridad durante la década 2009-2019.	● Seguridad, ● ciberseguridad, ● tendencias, ● amenazas, ● organización.	Los autores abordan los aspectos conceptuales, normativos y técnicos de la ciberseguridad, y ofrecen una visión actualizada de la situación.	Las organizaciones deben estar preparadas para afrontar las nuevas amenazas cibernéticas y adoptar medidas para proteger sus activos digitales
Auditorías en ciberseguridad: un modelo de aplicación general para empresas y naciones	● El documento presenta un modelo de auditoría de ciberseguridad aplicable a cualquier organización o nación, independientement e de su tamaño o sector.	Auditoría de ciberseguridad, modelo de auditoría ciberseguridad, seguridad de la información.	El modelo es una herramienta valiosa para las organizaciones que buscan evaluar su nivel de madurez en ciberseguridad. El modelo también puede ser utilizado por las naciones para evaluar su preparación frente a las amenazas cibernéticas.	El documento concluye que el modelo propuesto es una herramienta eficaz para la evaluación de la ciberseguridad. El modelo es aplicable a cualquier organización o nación, y puede ayudar a mejorar la seguridad de los sistemas y las redes.
Los desafíos de la ciberseguridad en Chile	● El documento destaca que la ciberseguridad es un tema cada vez más importante, ya que Chile depende cada vez más de las tecnologías digitales.	Ciberseguridad, Chile, desafíos, amenazas, respuesta.	Los autores abordan los aspectos conceptuales, normativos y técnicos de la ciberseguridad, y ofrecen una visión actualizada de la situación en Chile	El documento concluye que Chile debe fortalecer su capacidad de respuesta a las amenazas cibernéticas.
Riesgos de ciberseguridad en las empresas	El documento destaca que los riesgos de ciberseguridad son cada vez más graves y sofisticados.	● Ciberseguridad , ● empresas, ● riesgos, ● amenazas, ● impactos.	El documento proporciona un análisis completo de los principales riesgos de ciberseguridad a	El documento concluye que las empresas deben tomar medidas para mitigar los

			los que se enfrentan las empresas.	riesgos de ciberseguridad
Análisis de ciberseguridad sobre las vulnerabilidades que se pueden presentar con el teletrabajo	● El documento analiza las vulnerabilidades de ciberseguridad que se pueden presentar con el teletrabajo.	Ciberseguridad, teletrabajo, vulnerabilidades, amenazas, medidas.	Los autores abordan los aspectos conceptuales, normativos y técnicos de la ciberseguridad, y ofrecen una visión actualizada de la situación.	Se les debe proporcionar a los empleados formación en ciberseguridad, incluyendo el uso de dispositivos personales para el trabajo, la conexión a redes domésticas o públicas y la protección de la información confidencial.

RESULTADOS

La ciberseguridad en el contexto internacional

En principio, la revisión de la literatura arrojó una noción de *ciberseguridad* que es la que se toma como referente para los textos analizados. De esta manera, se define como "el conjunto de acciones, políticas, medidas y procedimientos de carácter técnico, organizativo y legal, que se aplican para proteger la infraestructura crítica, los sistemas informáticos, las redes de comunicación y la información contenida en ellos, de amenazas o ataques provenientes del mundo digital" (1).

Evidentemente, la gran revolución del siglo XXI, sin contar la inteligencia artificial, es el Internet. El ciberespacio es todo un hito en la existencia humana; no obstante, también trajo consigo toda una serie de riesgos y amenazas, que simplemente eran inimaginables hace apenas unas décadas, como se menciona a continuación.

En lo que respecta a los Estados, las amenazas como la guerra o las crisis económicas siguen latentes, sin embargo, la penetración de la Internet en el funcionamiento de los países expone a los gobiernos, empresas y ciudadanos a diferentes peligros en diferentes escalas.

Se identifica que el Internet mismo es una amenaza para la seguridad humana (2), ya que el auge de este ha puesto en cuestión muchas normas y aproximaciones sociopolíticas, incluyendo la forma de pensar la privacidad, la seguridad o los riesgos. Todo ello implica que haya modos distintos de pensar

la guerra, la privacidad, los riesgos, los conflictos o las libertades civiles y cómo podemos ajustarlas para garantizar los derechos civiles y la paz en la arena internacional.

Por otra parte, los principales ataques identificados que sufren tanto personas como organizaciones son el *phishing*, *ransomware*, *vishing*, *smishing, cryptojacking*, los Estados sufren ciberataques masivos y mucho más complejos principalmente (1-2-3-4-5).

En el Gobierno, se pueden identificar algunas acciones que podrían ser implementadas, basadas en cinco áreas esenciales para evaluar el compromiso con la ciberseguridad: medidas legales, técnicas y organizativas, formación y estandarización. Al respecto, diversos recursos consultados coinciden en que se requiere una mayor cooperación entre los países para desarrollar una metodología de evaluación más exhaustiva y confiable.

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos creó el Marco de la Fuerza Laboral de Ciberseguridad de la Iniciativa Nacional para la Educación en Ciberseguridad (NICE) (4), el cual gira en torno a cinco funciones:

Función	**Descripción**
1.Identificar (ID)	Define el conocimiento organizativo para gestionar el riesgo a la ciberseguridad de los sistemas, recursos, datos y capacidades.
2.Proteger (PR)	Establece e implementa las debidas salvaguardias para asegurar la prestación de servicios de infraestructura críticos.
3.Detectar (DE)	Establece e implementa actividades apropiadas para detectar la ocurrencia de un evento de ciberseguridad.
4.Responder (RS)	Establece e implementa las actividades correspondientes para tomar medidas en relación con un evento de ciberseguridad detectado.
5.Recuperar (RC)	Establece e implementa actividades apropiadas para mantener los planes de resiliencia y restaurar las capacidades o los servicios que se hayan visto afectados debido a un evento de ciberseguridad.

Análogamente, Naciones Unidas presenta un compendio en el cual se muestra la caracterización de las principales modalidades de ciberdelincuencia y los métodos y estrategias utilizados por los ciberdelincuentes (5). En este documento se concluye que es necesario que los Estados inviertan en la conformación de organismos especializados en enfrentar estas problemáticas y el sector privado está llamado a trabajar en la concientización del personal sobre lo real de estas amenazas.

De manera paralela, la ciberseguridad se manifiesta como un tópico recurrente, puesto que los ataques cibernéticos se han convertido en una de las principales amenazas a la seguridad internacional. Estos ataques pueden tener un impacto significativo en las infraestructuras críticas, los sistemas financieros y la estabilidad política de los países (6).

La ciberseguridad en Colombia

A nivel regional, diversos Estados, entre ellos Colombia, ya desarrollan una serie de estrategias encaminadas a garantizar una ciberseguridad fuerte. Estas estrategias se cristalizan en tres objetivos: protección de la infraestructura crítica, protección de las personas y las organizaciones y protección de la soberanía nacional (7). Al igual que se recalca la necesidad de la cooperación internacional.

Colombia, de cara al contexto global, afronta las problemáticas mencionadas. Sin embargo, como país presenta desafíos particulares, entre los que se incluyen deficiente nivel de concienciación frente a la ciberseguridad, a nivel individual y organizacional; escasa inversión en ciberseguridad a nivel empresarial y gubernamental y el aumento en la cantidad y sofisticación de los ciberataques de los que es víctima (8).

La falta de conciencia frente a los riesgos que representa la conectividad en el país puede explicarse por varios factores. En primer lugar, se ubica el escaso nivel de conciencia explicado en parte por la complejidad de los ciberataques; en segundo lugar, se encuentra la falta de inversión, que responde al elevado costo que representan las herramientas para defenderse de estos ataques; en tercer lugar, se encuentra la falta de comprensión de los beneficios de contar con sistemas de ciberdefensa robustos y que está directamente relacionada con el cuarto factor, que es el no ver la ciberseguridad como una prioridad (9).

La ciberseguridad en las empresas y en el mundo laboral

Un porcentaje de los documentos revisados presenta una definición de conceptos relacionados con la ciberseguridad, que a su vez desempeñan un papel importante en esta área. Así pues, conceptos como internet de las cosas, computación en la nube, computación móvil, convergencia tecnológica, aparecen en escena como nuevos elementos en disputa contra el cibercrimen (10).

Análogamente, se considera que la ciberseguridad debe cumplir con al menos tres requisitos: confidencialidad, integridad y disponibilidad (11). No obstante, se reconoce que la administración del Estado tiene la responsabilidad de tomar todas las medidas razonables para proteger sus sistemas de información, de las empresas y de los ciudadanos de los ciberataques, y que es responsable de los daños que resulten de un incidente de ciberseguridad.

Estos conceptos han emergido en la segunda década del siglo presente, y tienen impacto real en las personas y las organizaciones. Por ejemplo, el internet de las cosas extiende la conectividad a casi todos los electrodomésticos, la computación en la nube implica una pérdida del control de la información una vez se comparte y la convergencia tecnológica correlaciona mayor innovación con mayor riesgo.

Paralelamente, uno de los documentos consultados propone un modelo de auditoría de ciberseguridad (CSAM), que puede utilizarse para evaluar la madurez de la ciberseguridad de cualquier organización. El CSAM incluye 18 dominios, cada uno de los cuales tiene un número de subdominios y controles. El modelo puede utilizarse para realizar una auditoría integral de la postura de ciberseguridad de una organización, o puede utilizarse para centrarse en áreas específicas de preocupación (12).

Lo expuesto es fundamental si se considera que la información es el activo más importante con el que cuentan las empresas. Y esta puede ser comprometida de varias maneras, incluyendo ataques de *malware*, ataques de *phishing* y ataques de denegación de servicio (13).

Al respecto, el personal generalmente es el eslabón más débil en las organizaciones con respecto a la ciberseguridad (14), por lo que es importante crear una cultura de ciberseguridad dentro de la organización. Esto significa que todos en la organización, desde el CEO hasta el empleado de primera línea, deben ser conscientes de la importancia de la ciberseguridad y tomar medidas para proteger los datos y sistemas de la organización.

A nivel individual, el 2020 modificó muchos aspectos de la vida y el trabajo no fue la excepción. El teletrabajo es un fenómeno que se masificó luego de la pandemia. No obstante, también trae riesgos

a la seguridad, como el uso de dispositivos personales, conexiones inseguras y, por supuesto, escasa concienciación de los empleados frente a estos riesgos (15).

DISCUSIÓN

Medina (1) destaca la importancia de la ciberseguridad en la era actual y la define como un conjunto de acciones para proteger infraestructuras críticas y datos de amenazas digitales. Rodríguez Prieto (2), por su parte, argumenta que Internet cuestiona normas sociopolíticas, incluyendo la privacidad, y plantea desafíos a la seguridad humana.

Paralelamente, Morán (3) y Newhouse *et al.* (4) coinciden en que las amenazas cibernéticas, como el *phishing*, *ransomware* y los ciberataques masivos, afectan tanto a individuos como a organizaciones. Morán (3) sugiere que los gobiernos deben aplicar medidas legales, técnicas organizativas para abordar estas amenazas, mientras que Newhouse *et al.* (4) se centran en la importancia de la educación en ciberseguridad a través de la NICE.

Carlini (6) aboga por la cooperación internacional en ciberseguridad y argumenta que es un desafío para la comunidad internacional. Por otro lado, Leiva (7) se centra en estrategias nacionales de ciberseguridad y propone un enfoque comparativo basado en pasar de una visión global a una visión local. Este debate refleja la importancia de la cooperación internacional y las estrategias nacionales en la lucha contra las amenazas cibernéticas.

En Colombia, Ospina Díaz y Sanabria Rangel (8) destacan desafíos específicos en ciberseguridad, como la falta de concienciación, la escasa inversión y la sofisticación de los ciberataques. Además, Medina Ochoa (9) recalca que la seguridad en el ciberespacio es un desafío para Colombia. Cano (10) menciona conceptos emergentes, como internet de las cosas y la computación en la nube, que están relacionados con la ciberseguridad. Esto resalta la importancia de abordar desafíos específicos a nivel nacional en el contexto de la ciberseguridad.

La seguridad de la información y la concienciación son temas clave, como mencionan Santiago y Sánchez Allende (13) y García Forero (14). Santiago y Sánchez Allende (13) ponen de manifiesto los riesgos de ciberseguridad en las empresas, mientras que García Forero (14) destaca la importancia de

considerar al personal como una fuente potencial de riesgo. Estos puntos de vista subrayan la importancia de la educación y la cultura de ciberseguridad tanto a nivel organizacional como individual. En síntesis, la ciberseguridad es un tema crucial en el siglo XXI, con diversos enfoques y desafíos planteados por los expertos. La cooperación internacional, las estrategias nacionales y la concienciación son elementos esenciales en la lucha contra las amenazas cibernéticas, mientras que Colombia enfrenta desafíos particulares en este contexto. La seguridad de la información y la cultura de ciberseguridad se perfilan como factores fundamentales para mitigar riesgos en un entorno cada vez más digital.

La situación general

La falta de conciencia en ciberseguridad tanto a nivel individual como organizacional se debe a diversos factores, incluyendo la complejidad de las amenazas cibernéticas y la falta de educación pública sobre este tema (9-13). Frecuentemente, las personas carecen de información adecuada acerca de las mejores prácticas para proteger sus datos y sistemas (13). La educación y la concienciación son fundamentales para empoderar a la sociedad en la lucha contra las amenazas cibernéticas (14).

Además, es común que muchas personas subestimen la posibilidad de ser objeto de un ataque cibernético, lo que lamentablemente conduce a la negligencia en la implementación de medidas de seguridad y en la protección de datos personales y empresariales, de acuerdo con Medina *et al.* (9). La falta de conciencia en ciberseguridad se erige como una amenaza invisible que acecha tanto a individuos como a organizaciones, amenazando con su destrucción. Las brechas de seguridad actúan como herramientas que ponen en peligro la privacidad y la seguridad según Medina *et al.* (9).

Entre las creencias que influyen en la percepción de seguridad, se incluyen la idea de que “no soy el objetivo”, la falsa creencia de que “el *malware* solo afecta a sistemas Windows”, la confianza en que “la infraestructura existente garantiza inmunidad” y la errónea suposición de que “la seguridad de la información es un asunto exclusivo del departamento de TI” (9-13). A nivel empresarial, se destaca la necesidad de invertir tiempo y recursos en la capacitación del personal, ya que se reconoce que este constituye el eslabón más vulnerable en términos de estrategias de ciberseguridad (14).

En el contexto organizacional, existen creencias que, de ser mantenidas, pueden tener consecuencias perjudiciales para el valioso activo que representa la información (9-13), por lo cual la auditoría en ciberseguridad se presenta como una herramienta útil para hacer frente a las amenazas latentes en el ciberespacio (11). Este análisis subraya la importancia crucial de la educación y la sensibilización en materia de ciberseguridad, así como la urgente necesidad de eliminar creencias erróneas que pueden poner en riesgo la seguridad de la información tanto a nivel individual como en el entorno organizacional.

El ámbito laboral

La ciberseguridad es un desafío crítico para las empresas, y esto se manifiesta en su exposición a diversas amenazas cibernéticas. La falta de una sólida cultura de ciberseguridad en las organizaciones es un factor fundamental en este escenario, como se ha destacado en el estudio de Medina (1). Las amenazas persistentes, como el *vishing*, *phishing* y *smishing*, continúan siendo una preocupación vigente para las empresas, lo que subraya la necesidad apremiante de promover la conciencia y las prácticas de seguridad cibernética en todos los niveles de la organización.

Si bien las certificaciones otorgadas por organismos certificadores privados pueden ser valiosas herramientas para prevenir ciberdelitos, como se señala en Santiago y Sánchez (13), es fundamental comprender que no son una solución completa por sí mismas. Estas certificaciones deben ir de la mano con una responsabilidad individual asumida por cada empleado dentro de la organización. Esto implica que la seguridad cibernética no es únicamente un tema de papel, sino una mentalidad y una práctica que deben ser adoptadas en toda la empresa.

La educación emerge como un pilar esencial en una estrategia de ciberseguridad exitosa, como se destaca de manera reiterada en las investigaciones. El auge del teletrabajo plantea desafíos adicionales, ya que los empleados pasan largos períodos conectados, interactuando con numerosos sitios y aplicaciones “novedosas”. Estos comportamientos aumentan el riesgo de ser víctimas de ataques cibernéticos, lo que enfatiza la necesidad de una educación constante y en curso para sensibilizar a los empleados sobre los riesgos y promover prácticas seguras en línea.

Las medidas de mitigación, como proporcionarles a los empleados dispositivos y *software* seguros, así como monitorear las actividades en la red corporativa, son esenciales para reducir los riesgos cibernéticos, como se indica en las investigaciones. Estas acciones reflejan el compromiso de la organización con la seguridad de la información y la protección de sus activos, lo que es crucial en un entorno digital cada vez más amenazante.

En resumen, la ciberseguridad no puede ser subestimada por ninguna empresa que aspire a su supervivencia a largo plazo, como se menciona en las fuentes proporcionadas. La información es un activo valioso que debe protegerse de amenazas como el *malware*, los ataques de *phishing* y los ataques de denegación de servicio. La implementación de planes de acción efectivos para responder a posibles ataques cibernéticos es esencial para salvaguardar la integridad y la confidencialidad de los datos empresariales (1- 13).

CONCLUSIONES

Dadas las limitaciones de este estudio, no se muestran conclusiones definitivas frente a un tema que se encuentra en constante evolución. Se muestran posibles líneas de investigación que pueden ser profundizadas por investigadores interesados en el tema de la seguridad de la información y la ciberseguridad.

Se determina que, desde una perspectiva nacional, la infraestructura crítica de un país, como las redes eléctricas, sistemas de transporte y servicios de salud, está interconectada digitalmente. Un ataque cibernético exitoso a estos sistemas podría paralizar una nación entera, lo que subraya la importancia de proteger estos activos vitales para la seguridad y la estabilidad de una nación.

Análogamente, para las personas la ciberseguridad es esencial para proteger la privacidad y la seguridad financiera. Los ataques cibernéticos pueden llevar al robo de identidad, al acceso no autorizado a cuentas bancarias y al acoso en línea, lo que puede extenderse a la seguridad de las empresas, si estas no tienen prácticas adecuadas de protección de la información.

La falta de conciencia y prácticas de seguridad puede dejar a las personas vulnerables a estas amenazas, lo que destaca la importancia de la educación en ciberseguridad y la adopción de buenas prácticas para protegerse en el mundo digital actual.

Según lo expuesto, sería conveniente abrir una línea de investigación en el ámbito de las ciencias humanas como la antropología y la psicología, dada la necesidad de comprender las razones que subyacen en el inconsciente de las personas para negarse a adoptar medidas para su propia protección, aun teniendo abundante información al respecto.

En resumen, la ciberseguridad es una prioridad crítica en el mundo actual, ya que afecta a la seguridad nacional, la viabilidad de las empresas y la protección de la información y la privacidad de las personas. Finalmente, se concluye cómo las estrategias de ciberseguridad nos conciernen a todos, es un proceso que nunca va a estar acabado, ni es responsabilidad exclusiva de expertos en tecnología y seguridad. Asimismo, inversión y educación deben marchar de la mano, ya que desarrollar una estrategia efectiva de ciberseguridad, requiere contar con las herramientas adecuadas y la formación que permita evidenciar el peligro.

REFERENCIAS BIBLIOGRÁFICAS

1 Castillo Medina CA. Ciberseguridad: por dónde Empezar… Rev. de Tecnol. 2019; 18(1): 89-100.

2 Rodríguez Prieto R. ¿Qué seguridad? Riesgos y amenazas de Internet en la seguridad humana. Araucaria. 2016; 18(36): 391-415.

3 Morán Ramírez D. La visión internacional de la ciberseguridad. Pre-bie3. 2015; 2:15.

4 Newhouse W, Keith S, Scribner B, Witte G. Iniciativa nacional para la educación en ciberseguridad (NICE): Marco para el personal de ciberseguridad [Internet]. Maryland: National Institute of Standards and Technology; 2020. NIST Special Publication (SP) 800: 181.160 p. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

5 Oficina de Naciones Unidas Contra la Droga y el Delito. Compendio de ciberdelincuencia organizada. Viena: Oficina de las Naciones Unidas en Viena; 2022.

6 Carlini A. Ciberseguridad: un nuevo desafío para la comunidad

internacional. IEEE Doc Opin. 2016;(67):1-16.

7 Leiva EA. Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Rev Latinoam Ing Softw. 2015; 3(4):161-176.

8 Ospina Díaz MR, Sanabria Rangel PE. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Rev Crim* 2020; 62(2): 199-217.

9 Medina Ochoa GE (Ed.). La seguridad en el ciberespacio: un desafío para Colombia. 2.ª ed. Bogotá: Escuela Superior de Guerra; 2022.

10 Cano JJ. Seguridad y ciberseguridad 2009-2019. Rev Sist 2020; 155: 81-94.

11 Sabillón R, Cano JJ. Auditorías en ciberseguridad: Un modelo de aplicación general para empresas y naciones. Rev Ibér de Sist Tecnol Inform. 2019; (32): 33-48.

12 Álvarez Valenzuela D. Los desafíos de la ciberseguridad en Chile. Rev Chil Der Tecnol. 2017; 6(2): 1-2.

13 Santiago EJ, Sánchez Allende J. Riesgos de ciberseguridad en las empresas. *Tecnología Desarro.* 2017; 15:10.

14 García Forero L. Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. Universidad Piloto de Colombia [Internet]; 2020 [consultado el 31 de octubre de 2023]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9545/Ciberseguridad%20en%20las%20organizaciones%2C%20el%20personal.pdf?sequence=1&isAllowed=y

15 Arévalo Morales AD, Buitrago Ropero CA. Análisis de ciberseguridad sobre las vulnerabilidades que se pueden presentar con el teletrabajo [tesis de especialización; impresa]. [Bogotá]: Fundación Universitaria Los Libertadores; 2022. 18 p.